Ambassador Daniel Sepulveda
Remarks on the U.S. Privacy Framework
and the Consumer Privacy Bill of Rights
May 13, 2015, 9:00am
Foundation for Legal and Business Research (FIDE)
Madrid, Spain

Thank you for the opportunity to join you to present an overview of the American approach to protecting personal privacy in commerce and for the opportunity to exchange perspectives on how that approach has evolved as well as how it compares to and can be interoperable with the European approach to the same challenge.

Our existing privacy protections in law and practice are strong. They are built on a history of commitment to the dignity of the individual and strong protections against improper collection, use, or distribution of personal information.

Consumers benefit from legal protection barring deceptive or unfair business practices combined with robust enforcement by our consumer protection agencies, binding contracts between companies that process data, market pressure from customers on firms, social pressure from privacy activists on those using information, and vigilance by a free press.

Together, those forces create a holistic environment of protection for privacy that provides consumers with strong privacy protections and innovative digital services. Leading American firms have chief privacy officers and other trained privacy professionals, as well as coordinated policies and practices, to ensure the trust and confidence of the people they serve. These professionals help ensure that American entities' privacy practices evolve to reflect ever-changing technologies and practices.

Nonetheless, this Administration has explored how we can do better, both as a matter of law and practice. In response to that challenge, the Federal Trade Commission and the Department of Commerce have issued multiple reports, engaged with stakeholders on how a combination of laws and voluntary practices can help ensure that people have the information and tools necessary to protect their dignity and information in the digital age.

Further, President Obama directed John Podesta to lead a scoping exercise to identify privacy challenges in the age of "Big Data"-an effort that resulted in

multiple private and public sector reforms as well as the February release of a potential framework for a Consumer Privacy Bill of Rights. The draft law would provide greater specificity and certainty to consumers as to what they can expect from those who collect, use, and share their information.

In his release of the Administration's proposed framework for a Consumer Privacy Bill of Rights, President Obama states, "even though we live in a world where we share personal information more freely than in the past, we must reject the notion that privacy is an outdated value. It has been at the heart of our democracy since its inception, and we need it now more than ever."

It is that commitment, coupled with the Administration's efforts to enable and encourage innovation, that has led us to take a measured, thoughtful, and inclusive approach to determine how to best tackle privacy protection in the digital age. Getting the policies and practices right are critical to both individual autonomy as well as the future of the global economy.

We are sometimes met with skepticism in Europe about our commitment to privacy in America because we lack an overarching law on commercial privacy. FTC Commissioner Julie Brill, a leading mind on these issues, has pushed back on that criticism in expert fashion, outlining the authorities of the FTC's power to protect consumers as well as the U.S. laws that govern privacy in specific business areas like health care and financial services. I refer you to her various speeches on the subject, many of which were made here in Europe.

Nonetheless, we recognize and agree with those in the privacy community that gaps remain in the fabric of privacy protection in our market and that consumers at home and regulators abroad are asking us to do better. That is a rational request given the rising complexity of networks, diversity of services, cybersecurity threats, and incidents of identity theft. Recent polls show that 9 in 10 Americans feel they have in some way lost control of their personal information — and that can lead to less interaction with technology, less innovation, and a less productive economy.

The President understands, and we believe industry does as well, that we have to work together to create a continually improving environment of respect for people's personal information in order to support the trust necessary to encourage use of services and promote the continued growth of the digital economy.

At the Federal Trade Commission earlier this year, President Obama presented his

comprehensive approach to enhancing that trust by improving consumers' security, tackling identity theft, and bolstering privacy online and in the classroom.

Among his proposals, the President has put forward a new legislative proposal to help bring peace of mind to the tens of millions of consumers whose personal and financial information has been compromised in a data breach. This proposal clarifies and strengthens the obligations companies have to notify customers when their personal information has been exposed, including establishing a 30-day notification requirement from the discovery of a breach, while providing companies with the certainty of a single, national standard. The proposal also criminalizes illicit overseas trade in stolen identities.

To further address identity theft, the President has sought to give consumers access to one of the best early indicators of identity theft, as well as an opportunity to improve their credit health. JPMorganChase and Bank of America, in partnership with Fair Isaac Corporation (FICO), will join the growing list of firms making credit scores available for free to their consumer card customers. USAA and State Employees' Credit Union will also offer free credit scores to their members, and Ally Financial is further widening the community of companies taking this step by making credit scores available to their auto loan customers. Through this effort more than half of all adults in the U.S. with credit scores will now have access to this tool to help spot identity theft.

To protect students, the President has released a legislative proposal designed to provide teachers and parents the confidence they need to enhance teaching and learning with the best technology — by ensuring that data collected in the educational context is used only for educational purposes. This bill, modeled on a landmark California statute, builds on the recommendations of the White House Big Data review released earlier this year, would prevent companies from selling student data to third parties for purposes unrelated to educational missions and from targeting advertising to students based on data collected in school – while still permitting important research initiatives to improve student learning outcomes, and efforts by companies to continuously improve the effectiveness of their learning technology products.

Not wanting to wait for a law to pass, the President won new commitments from the private sector to help enhance students' privacy on the day he announced the legislative proposal. Seventy-five companies have committed to the cause, signing a pledge to provide kids, parents, and teachers with important protections against misuse of their data.

And on top of all that work, the Administration issued its legislative draft of the Consumer Privacy Bill of Rights, calling on stakeholders, Congress, and individuals to discuss and work toward a comprehensive framework for privacy protection that is flexible, understandable, and beneficial to consumers and industry alike.

The Consumer Privacy Bill of Rights applies to *personal data*, which means any data, including aggregations of data, that is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device. Even without legislation, the Administration will continue to convene multistakeholder processes that use this Bill of Rights as a template for codes of conduct that are enforceable by the Federal Trade Commission. These elements—the Consumer Privacy Bill of Rights, codes of conduct, and strong enforcement—we believe will increase interoperability between the U.S. consumer data privacy framework and those of our international partners.

The Consumer Privacy Bill of Rights is derived from the Fair Information Practices Principles – principles that have long been the basis for privacy protections in the U.S., Europe, and around the world. We are committed to ensuring that consumers benefit from:

INDIVIDUAL CONTROL: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

TRANSPARENCY: Consumers have a right to easily understandable and accessible information about privacy and security practices. At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it, and whether and for what purposes they may share personal data with third parties.

RESPECT FOR CONTEXT: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide

heightened Transparency and Individual Control by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults.

SECURITY: Consumers have a right to secure and responsible handling of personal data. Companies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.

ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.

FOCUSED COLLECTION: Consumers have a right to reasonable limits on the personal data that companies collect and retain. Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise.

ACCOUNTABILITY: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights. Companies should be accountable to enforcement authorities and consumers for adhering to these principles.

Now, at the same time as we proposed changes to our laws and practices, our Department of Commerce has been engaged with European officials on updating the Safe Harbor Framework for commercial data transfers.

The Safe Harbor's 4,000 plus membership is as deep and broad as the U.S.-EU

relationship. Safe Harbor companies come from almost every sector of the economy and include both U.S.-headquartered companies and the U.S. subsidiaries and affiliates of EU-headquartered companies. In addition to the thousands of companies in Safe Harbor, countless EU-based companies rely on the Framework to conduct business with their U.S.-based partners and clients.

U.S. and EU companies have built one of the most robust cross-border data networks in the world. Safe Harbor strengthens and facilitates this network, which is a critical pillar of our competitiveness. Safe Harbor also provides vital privacy protections to the benefit of EU citizens, most importantly through the strong enforcement of the U.S. Federal Trade Commission.

We believe in the program and are proud of it. Nonetheless, we took the European Commission's November 2013 report on Safe Harbor very seriously, and the Department of Commerce has worked hard alongside the Commission over the past year and a half to address the issues raised. My colleagues have leaned far forward in their response to the Commission in an effort to bring the consultations to a successful conclusion as soon as possible to remove the uncertainty that has been created for businesses and citizens on both sides of the Atlantic.

We are confident that we will be able to reach an agreement that enables Safe Harbor to continue serving its intended purposes protecting privacy and facilitating transatlantic trade and investment. We are also confident that our Trans Atlantic friendship and cooperation based on shared values will remain strong.

We look forward to working with you and I appreciate your time.